- (i) determining whether the intercepted DNS request corresponds to a secure server;
- (ii) when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and
- (iii) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.
- 83. The data processing device of claim 82, wherein step (iii) comprises the steps of:
  - (a) determining whether the client is authorized to access the secure server; and
  - (b) when the client is authorized to access the secure server, sending a request to the secure server to establish an encrypted channel between the secure server and the client.
- 84. The data processing device of claim 83, wherein step (iii) further comprises the step of:
  - when the client is not authorized to access the secure server, returning a host unknown error message to the client.
- 85. The data processing device of claim 84, wherein the client comprises a web browser into which a user enters a URL resulting in the DNS request.

- 86. A data processing device, comprising memory storing a domain name server (DNS) proxy module that intercepts DNS requests sent by a client and, for each intercepted DNS request, when the intercepted DNS request corresponds to a secure server, determines whether the client is authorized to access the secure server and, if so, automatically initiates an encrypted channel between the client and the secure server.
- 87. A computer readable medium storing a domain name server (DNS) proxy module comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:
  - (i) intercepting a DNS request sent by a client;
  - (ii) determining whether the intercepted DNS request corresponds to a secure server;
  - when the intercepted DNS request does not correspond to a secure server, forwarding the DNS request to a DNS function that returns an IP address of a nonsecure computer; and
  - (iv) when the intercepted DNS request corresponds to a secure server, automatically initiating an encrypted channel between the client and the secure server.
  - 88. The computer readable medium of daim 87, wherein step (iii) comprises the steps of:
    - (a) determining whether the client is authorized to access the secure server; and
    - (b) when the client is authorized to access the secure server, sending a request to the secure server to establish an encrypted channel between the secure server and the client.

- 89. The computer readable medium of claim 88, wherein step (iii) further comprises the step of:
  - when the client is not authorized to access the secure server, returning a host unknown extror message to the client.
- 90. The computer readable medium of claim 89, wherein the client comprises a web browser into which a user enters a URL resulting in the DNS request.
- 91. A computer readable medium comprising computer readable instructions that, when executed, cause a domain name server (DNS) proxy module to intercept DNS requests sent by a client and, for each intercepted DNS request, when the intercepted DNS request corresponds to a secure server, determines whether the client is authorized to access the secure server and, if so, automatically initiates an encrypted channel between the client and the secure server.

## Remarks

Applicants have added new claims 82 - 91 to more completely claim the disclosed invention. Support for the new claims may be found at least on pages 59-60 and in FIG. 26.